REMARKS

Claims 1-35, 69-79, 88, 89-91 are pending. Claims 1, 69, 88, and 89 are in independent form.

Rejections under 35 U.S.C. § 103(a)

Claim 1 was rejected under 35 U.S.C. § 103(a) as obvious over U.S. Patent No. 6,477,651 to Teal et al. (hereinafter "Teal") and U.S. Patent No. 6,988,208 to Hrabik et al. (hereinafter "Hrabik").

Claim 1 relates to a machine-implemented method for automatically identifying new signatures to use in identifying a previously unknown intrusive network attack. The method includes obtaining a collection of data items to be analyzed to identify the network attack, wherein said data items are parts of messages that were sent over a data network, reducing said data items in said collection to reduce said data collection to a reduced data collection of reduced data items, analyzing a plurality of said reduced data items to detect common elements in the plurality of said reduced data items, said analyzing identifying common content indicative of the previously unknown network attack, and sending the common content to one or more of a signature blocker and a signature manager.

The reduced data items in the reduced data collection have a smaller size and a constant predetermined relation with data

items in the data collection and at least some of the data items in the data collection that differ are reduced to the same reduced data item.

The rejection of claim 1 contends that it would have been obvious for one of ordinary skill to have combined Teal and Hrabik and to have arrived at the recited subject matter.

Applicant respectfully disagrees for several reasons. As a threshold matter, claim 1 relates to a method for automatically identifying new signatures to use in identifying a previously unknown intrusive network attack. Further, the method includes sending common content identified by analyzing a plurality of reduced data items to one or more of a signature blocker and a signature manager.

Teal and Hrabik neither describe nor suggest these features. Indeed, Teal and Hrabik both describe systems that necessarily operate with old signatures of known network attacks. For example, Teal describes the modification of intrusion detection systems to adapt to new network vulnerabilities by upgrading it in a dynamic manner. *See, e.g., Teal*, col. 2, line 38-48. In particular, Teal's intrusion detection system 10 includes an intrusion detection analysis engine 16 that analyzes network data to look for specific patterns (i.e., "signatures") that indicate malicious activity on the network. *See, e.g., Teal*, only figure; col. 4, line 32-

35. Intrusion detection analysis engine 16 performs this analysis using analysis objects 18. *See, e.g., Teal*, col. 4, line 37-40. Each analysis object 18 provides dynamically loadable and unloadable executable code for identification of a signature associated with an attack on a network vulnerability. *See, e.g., Teal*, col. 4, line 41-43.

It is respectfully submitted that Teal's code for identification of a signature provided by analysis objects 18 must necessarily operate with old signatures of known network attacks. For example, it is only after a network vulnerability is found that a new analysis object can be developed. *See, e.g., Teal*, col. 5, line 9-11. Teal does not provide details regarding how the new signatures for such new analysis objects are identified. However, it is understood that the signatures cannot be new if the executable code of the analysis objects 18 for the identification a signature already exists.

Hrabik does not remedy these deficiencies in Teal. Indeed, even if Hrabik is understood to involve signatures in the identification of "security events," those signatures are understood to already be old signatures of known network attacks.

The rejection of claim 1, as best understood, relies on the contention that the collection and analysis of network data by Teal's intrusion detection system 10 describes the

identification of new signatures of unknown network attacks. Applicant respectfully disagrees. To being with, Teal himself considers the identification of new signatures, and the development of new analysis objects, to be separate from the collection and analysis of network data by intrusion detection system 10. In particular, Teal describes that new analysis objects can be developed and implemented by signature API 20. *See, e.g., Teal*, col. 5, line 9-22. However, the development and implementation of new analysis objects does not appear to receive any information from intrusion detection system 10. Indeed, Teal explicitly describes that third party developers can create new analysis objects. *See, e.g., Teal*, col. 4, line 43-47. Teal does not describe or suggest that the any information from intrusion detection system 10 is provided to these third party developers.

Indeed, since the creation of new analysis objects apparently takes place without any input from Teal's intrusion detection system 10, there is no reason to believe that patterns of malicious activity which are identified by Teal's intrusion detection system 10 are sent to one or more of a signature blocker and a signature manager, as is the common content identified by analyzing a plurality of reduced data items recited in claim 1.

The rejection of claim 1 also contends that Hrabik's combination of similar messages from different sources to reduce the level of redundancy in event data necessarily reduces data items, wherein the reduced data items in the reduced data collection have a smaller size and a constant predetermined relation with data items in the data collection and at least some of the data items in the data collection that differ are reduced to the same reduced data item.

Applicant respectfully disagrees for several reasons. Many of these reasons stem from the distinction between reducing data items (as recited) and Hrabik's combination of similar messages from different sources to reduce the size of the data base storing those messages.

In particular, while combining similar messages may reduce the size of a data base, it does not necessarily reduce the messages themselves. Indeed, it would appear that— absent some discarding of information— combining similar messages from different sources to reduce the level of redundancy will increase the size of a message. For example, suppose message A and message B were 80% redundant and 20% non-redundant. A "combination" of message A and message B could presumably retain the 80% redundant content as well as all of the non-redundant content. The total size of the combination would be larger (i.e., 80% redundant content + 20% non-redundant content from

message A + 20% non-redundant content from message B), even if the redundant information were discarded. The messages themselves would not be reduced. Instead, the size of the database holding those messages would be reduced.

This distinction is even more apparent when the subject matter recited in claim 1 is considered. For example, claim 1 recites that it is "the reduced data items in the reduced data collection [that] have a smaller size and a constant predetermined relation with data items in the data collection." Thus, it is not the reduced data collection that has a smaller size than the data collection of data items but rather the reduced data items that have a smaller size and a constant predetermined relation with data items in the data collection.

As another example, claim 1 recites that at least some of the data items in the data collection that differ are reduced to the same reduced data item. Combining multiple messages to yield a single larger message (as discussed above) does not reduce messages that differ to the same reduced data item. Instead, the combining multiple messages yields a message that has a large size than the starting messages.

Please note that Hrabik neither describes nor suggests that any of the information content (i.e., redundant content, non-redundant content, or otherwise) from the messages is discarded.

There thus does not appear to be any reduction of Hrabik's messages.

Accordingly, even if Teal and Hrabik were combined, one of ordinary skill would not arrive at the recited subject matter. Indeed, to the extent that Hrabik describes that messages are to be combined and hence increased in size, Hrabik can be seen as teaching away from the recited subject matter. Claim 1 is thus not obvious over Teal and Hrabik. Applicant respectfully requests that the rejections of claim 1 and the claims dependent therefrom be withdrawn.

Claim 69 was rejected under 35 U.S.C. § 103(a) as obvious over Teal, Hrabik, and U.S. Patent No. 7,089,592 to Adjaoute (hereinafter "Adjaoute").

Claim 69 relates to a machine-implemented method for automatically identifying new signatures to use in identifying a previously unknown intrusive network attack. The method includes monitoring network content on a network and obtaining at least portions of the data on said network, data reducing said portions of the data using a data reduction function which reduces said portions of the data to reduced data portions in a repeatable manner such that each portion which has the same content is reduced to the same reduced data portion and at least some of the portions that differ are reduced to the same reduced

data portion, analyzing said reduced data portions to find network content which repeats a specified number of times in order to establish said network content which repeats said specified number of times as frequent content, identifying address information of said frequent content, identifying the frequent content as associated with the previously unknown network attack based on said identifying and determining, and sending the frequent content to one or more of a signature blocker and a signature manager

The address information includes at least one of source information or destination information that characterizes the respective of sources and/or destinations of said frequent content and determining if a number of sources and/or destinations of said frequent content is increasing.

The rejection of claim 69 contends that it would have been obvious for one of ordinary skill to have combined Teal, Hrabik, and Adjaoute to have arrived at the recited subject matter.

Applicant respectfully disagrees for several reasons. As a threshold matter, claim 69 relates to a method for automatically identifying new signatures to use in identifying a previously unknown intrusive network attack. Further, the method includes sending frequent content that is identified as associated with a previously unknown network attack to one or more of a signature blocker and a signature manager.

Teal, Hrabik, and Adjaoute neither describe nor suggest these features. Instead, Teal, Hrabik, and Adjaoute all describe systems that necessarily operate with old signatures of known network attacks. Indeed, Adjaoute recognizes the distinction between signatures of new, previously unknown attacks and old signatures of known attacks. *See, e.g.*, *Adjaoute*, col. 2, line 52-57.

The rejection of claim 69 refers to the rejection of claim 1 and thus shares the same deficiencies discussed above. For example, the collection and analysis of network data by Teal's intrusion detection system 10 does not identify new signatures of unknown network attacks. Indeed, Teal and Adjaoute both consider the identification of new signatures, and (in Teal's case) the development of new analysis objects, to be separate from the collection and analysis of network data.

Further, since the creation of new analysis objects apparently takes place without any input from Teal's intrusion detection system 10, there is no reason to believe that patterns of malicious activity which are identified by Teal's intrusion detection system 10 are sent to one or more of a signature blocker and a signature manager, as is the frequent content that is identified as associated with a previously unknown network attack recited in claim 69.

The rejection of claim 69 also contends that Hrabik's combination of similar messages from different sources to reduce the level of redundancy in event data necessarily data reduces portions of data on a network using a data reduction function which reduces the portions of the data to reduced data portions in a repeatable manner such that each portion which has the same content is reduced to the same reduced data portion and at least some of the portions that differ are reduced to the same reduced data portion, as recited in claim 69.

Applicant respectfully disagrees for several reasons. Once again, many of these reasons stem from the distinction between reducing portions of data on a network (as recited) and Hrabik's combination of similar messages from different sources to reduce the size of the data base storing those messages.

In particular, while combining similar messages may reduce the size of a data base, it does not necessarily reduce the messages themselves. Indeed, it would appear that— absent some discarding of information— combining similar messages from different sources to reduce the level of redundancy will increase the size of a message.

This distinction is even more apparent when the subject matter recited in claim 69 is considered. For example, claim 69 recites that "at least some of the portions that differ are reduced to the same reduced data portion." However—absent some

discarding of information— Hrabik's combination of similar messages will result in a message that is increased in size.

Accordingly, even if Teal, Hrabik, and Adjaoute were combined, one of ordinary skill would not arrive at the recited subject matter. Indeed, to the extent that Hrabik describes that messages are to be combined and hence increased in size, Hrabik can be seen as teaching away from the recited subject matter. Claim 69 is thus not obvious over Teal, Hrabik, and Adjaoute. Applicant respectfully requests that the rejections of claim 69 and the claims dependent therefrom be withdrawn.

Claim 88 was rejected under 35 U.S.C. § 103(a) as obvious over Teal, Adjaoute, and Hrabik.

Claim 88 relates to a machine-implemented method for automatically identifying new signatures to use in identifying a previously unknown intrusive network attack. The method includes obtaining a collection of data items to be analyzed to identify the previously unknown network attack, reducing said data items in said collection to reduce said data collection to a reduced data collection of reduced data items, analyzing a plurality of said reduced data items to determine frequently occurring sections of message information indicative of a network attack, carrying out an additional test on said frequently occurring sections of message information, and based

on the additional test, sending some of the frequently occurring sections to one or more of a signature blocker and a signature manager.

The reduced data items in the reduced data collection have a smaller size and a constant predetermined relation with data items in the data collection and at least some of the data items in the data collection that differ are reduced to the same reduced data item.

Carrying out the additional test includes maintaining a first list of unassigned addresses, forming a second list of source addresses that have sent to the unassigned addresses on said first list, and comparing a current source of a frequently occurring section to said second list. The unassigned addresses are maintained as reduced addresses that have a smaller size and a constant predetermined relation with the unassigned addresses and at least some of the unassigned addresses that differ are reduced to the same reduced address. The source addresses are maintained as reduced addresses that have a smaller size and a constant predetermined relation with the source addresses and at least some of the source addresses that differ are reduced to the same reduced address.

The rejection of claim 88 contends that it would have been obvious for one of ordinary skill to have combined Teal, Hrabik, and Adjaoute to have arrived at the recited subject matter.

Applicant respectfully disagrees for several reasons. As a threshold matter, claim 88 relates to a method for automatically identifying new signatures to use in identifying a previously unknown intrusive network attack. Further, the method includes sending some of frequently occurring sections determined by analyzing a plurality of reduced data items to one or more of a signature blocker and a signature manager.

Teal, Hrabik, and Adjaoute neither describe nor suggest these features. Instead, Teal, Hrabik, and Adjaoute all describe systems that necessarily operate with old signatures of known network attacks. Indeed, Adjaoute recognizes the distinction between signatures of new, previously unknown attacks and old signatures of known attacks. *See, e.g., Adjaoute*, col. 2, line 52-57.

The rejection of claim 88 refers to the rejection of claim 1 and thus shares the same deficiencies discussed above. For example, the collection and analysis of network data by Teal's intrusion detection system 10 does not identify new signatures of unknown network attacks. Indeed, Teal and Adjaoute both consider the identification of new signatures, and (in Teal's case) the development of new analysis objects, to be separate from the collection and analysis of network data.

Further, since the creation of new analysis objects apparently takes place without any input from Teal's intrusion

detection system 10, there is no reason to believe that patterns of malicious activity which are identified by Teal's intrusion detection system 10 are sent to one or more of a signature blocker and a signature manager, as are some of the frequently occurring sections determined by analyzing a plurality of reduced data items recited in claim 88.

The rejection of claim 88 also contends that Hrabik's combination of similar messages from different sources to reduce the level of redundancy in event data necessarily reduces data items, wherein the reduced data items have a smaller size and a constant predetermined relation with data items in the data collection and at least some of the data items in the data collection that differ are reduced to the same reduced data item, as recited in claim 88.

Applicant respectfully disagrees for several reasons. Once again, many of these reasons stem from the distinction between reducing data items (as recited) and Hrabik's combination of similar messages from different sources to reduce the size of the data base storing those messages.

In particular, while combining similar messages may reduce the size of a data base, it does not necessarily reduce the messages themselves. Indeed, it would appear that— absent some discarding of information— combining similar messages from

different sources to reduce the level of redundancy will increase the size of a message.

This distinction is even more apparent when the subject matter recited in claim 88 is considered. For example, claim 88 recites that it is "the reduced data items in the reduced data collection [that] have a smaller size and a constant predetermined relation with data items in the data collection." Thus, it is not the reduced data collection that has a smaller size than the data collection of data items but rather the reduced data items that have a smaller size and a constant predetermined relation with data items in the data collection.

As another example, claim 88 recites that at least some of the data items in the data collection that differ are reduced to the same reduced data item. Combining multiple messages to yield a single larger message (as discussed above) does not reduce messages that differ to the same reduced data item. Instead, the combining multiple messages yields a message that has a large size than the starting messages.

Accordingly, even if Teal, Hrabik, and Adjaoute were combined, one of ordinary skill would not arrive at the recited subject matter. Indeed, to the extent that Hrabik describes that messages are to be combined and hence increased in size, Hrabik can be seen as teaching away from the recited subject matter. Claim 88 is thus not obvious over Teal, Hrabik, and

Adjaoute. Applicant respectfully requests that the rejections of claim 88 and the claims dependent therefrom be withdrawn.

Claim 89 was rejected under 35 U.S.C. § 103(a) as obvious over Teal, Adjaoute, and Hrabik.

Claim 89 relates to a machine-implemented method for automatically identifying new signatures to use in identifying a previously unknown intrusive network attack. The method includes obtaining a collection of data items to be analyzed to identify the network attack, reducing said data items in said collection to reduce said data collection to a reduced data collection of reduced data items, analyzing a plurality of said reduced data items to detect common elements, obtaining a second subset of the same network packet for subsequent analysis, and based on the subsequent analysis, sending some of the common content to one or more of a signature blocker and a signature manager. The data items comprise a first subset of a network packet including payload and header. The reduced data items in the reduced data collection have a smaller size and a constant predetermined relation with data items in the data collection and at least some of the data items in the data collection that differ are reduced to the same reduced data item. The analyzing reviews for common content indicative of a network attack.

The rejection of claim 89 contends that it would have been obvious for one of ordinary skill to have combined Teal, Hrabik, and Adjaoute to have arrived at the recited subject matter.

Applicant respectfully disagrees for several reasons. As a threshold matter, claim 89 relates to a method for automatically identifying new signatures to use in identifying a previously unknown intrusive network attack. Further, the method includes sending some of the common content reviewed for by analyzing a plurality of reduced data items to detect common elements to one or more of a signature blocker and a signature manager.

Teal, Hrabik, and Adjaoute neither describe nor suggest these features. Instead, Teal, Hrabik, and Adjaoute all describe systems that necessarily operate with old signatures of known network attacks. Indeed, Adjaoute recognizes the distinction between signatures of new, previously unknown attacks and old signatures of known attacks. *See, e.g., Adjaoute*, col. 2, line 52-57.

The rejection of claim 89 refers to the rejection of claim 1 and thus shares the same deficiencies discussed above. For example, the collection and analysis of network data by Teal's intrusion detection system 10 does not identify new signatures of unknown network attacks. Indeed, Teal and Adjaoute both consider the identification of new signatures, and (in Teal's

case) the development of new analysis objects, to be separate from the collection and analysis of network data.

Further, since the creation of new analysis objects apparently takes place without any input from Teal's intrusion detection system 10, there is no reason to believe that patterns of malicious activity which are identified by Teal's intrusion detection system 10 are sent to one or more of a signature blocker and a signature manager, as is some of the common content reviewed for by analyzing a plurality of reduced data items recited in claim 89.

The rejection of claim 89 also contends that Hrabik's combination of similar messages from different sources to reduce the level of redundancy in event data necessarily reduces data items, wherein the reduced data items have a smaller size and a constant predetermined relation with data items in the data collection and at least some of the data items in the data collection that differ are reduced to the same reduced data item, as recited in claim 89.

Applicant respectfully disagrees for several reasons. Once again, many of these reasons stem from the distinction between reducing data items (as recited) and Hrabik's combination of similar messages from different sources to reduce the size of the data base storing those messages.

In particular, while combining similar messages may reduce the size of a data base, it does not necessarily reduce the messages themselves. Indeed, it would appear that— absent some discarding of information— combining similar messages from different sources to reduce the level of redundancy will increase the size of a message.

This distinction is even more apparent when the subject matter recited in claim 89 is considered. For example, claim 89 recites that it is "the reduced data items in the reduced data collection [that] have a smaller size and a constant predetermined relation with data items in the data collection." Thus, it is not the reduced data collection that has a smaller size than the data collection of data items but rather the reduced data items that have a smaller size and a constant predetermined relation with data items in the data collection.

As another example, claim 89 recites that at least some of the data items in the data collection that differ are reduced to the same reduced data item. Combining multiple messages to yield a single larger message (as discussed above) does not reduce messages that differ to the same reduced data item. Instead, the combining multiple messages yields a message that has a large size than the starting messages.

Accordingly, even if Teal, Hrabik, and Adjaoute were combined, one of ordinary skill would not arrive at the recited

subject matter. Indeed, to the extent that Hrabik describes that messages are to be combined and hence increased in size, Hrabik can be seen as teaching away from the recited subject matter. Claim 89 is thus not obvious over Teal, Hrabik, and Adjaoute. Applicant respectfully requests that the rejections of claim 89 and the claims dependent therefrom be withdrawn.

It is believed that all of the pending claims have been addressed. However, the absence of a reply to a specific rejection, issue, or comment does not signify agreement with or concession of that rejection, issue, or comment. In addition, because the arguments made above may not be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Finally, nothing in this paper should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this paper, and the amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment.

Applicant asks that all claims be allowed. No fees are believed due at this time. Please apply any charges or credits, to deposit account 06-1050.

Respectfully submitted,

Date: October 9, 2009 /John F. Conroy, Reg. #45,485/
John F. Conroy
Reg. No. 45,485

Fish & Richardson P.C.
PTO Customer No. 20985
12390 El Camino Real
San Diego, California 92130
(858) 678-5070 telephone
(858) 678-5099 facsimile